



## FRONTESPIZIO DELIBERAZIONE

AOO: ausl\_fe  
REGISTRO: Deliberazione  
NUMERO: 0000044  
DATA: 28/02/2020 09:20  
OGGETTO: ADOZIONE DEL DOCUMENTO: "REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI NELL'AZIENDA USL DI FERRARA (REGOLAMENTO UE 2016/679 E D.LGS. 30.06.2003 N.196) E REVOCA DELLA PROPRIA PRECEDENTE DELIBERAZIONE N. 253 DEL 28.12.2018"

### SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Vagnini Claudio in qualità di Direttore Generale  
Con il parere favorevole di Natalini Nicoletta - Direttore Sanitario  
Con il parere favorevole di Carlini Stefano - Direttore Amministrativo

### CLASSIFICAZIONI:

- [01-01]

### DESTINATARI:

- Collegio sindacale
- UO SERVIZIO COMUNE TECNICO E PATRIMONIO
- UO SERVIZIO COMUNE FORMAZIONE E AGGIORNAMENTO
- UO SERVIZIO COMUNE ECONOMIA E GEST. CONTRATTI
- UO SERVIZIO COMUNE TECNOLOGIE DELLA COMUNICAZIONE E INFORMATICA
- UO SERVIZIO COMUNE GESTIONE PERSONALE
- UO SERVIZIO ASSICURATIVO COMUNE E DEL CONTENZIOSO
- UO SERVIZI AMMINISTRATIVI DISTRETTUALI
- UO SERVIZI AMMINISTRATIVI PUO
- DIPARTIMENTO CURE PRIMARIE
- DIPARTIMENTO SANITA PUBBLICA
- DIPARTIMENTO ASS. INT. SALUTE MENTALE DP
- DIPARTIMENTO DIREZIONE ASS. ZA OSPEDALIERA
- DAI - DIPARTIMENTO DI MEDICINA
- DAI - DIPARTIMENTO DI CHIRURGIA
- DAI - DIPARTIMENTO MATERNO INFANTILE
- DAI -DIPARTIMENTO DI EMERGENZA
- DAI - DIPARTIMENTO RADIOLOGIA
- DAI - DIPTO BIOTECNOLOGIE -TRASFUSIONALE E DI LABORATORIO



L'originale del presente documento, redatto in formato elettronico e firmato digitalmente e' conservato a cura dell'ente produttore secondo normativa vigente.

Ai sensi dell'art. 3bis c4-bis Dlgs 82/2005 e s.m.i., in assenza del domicilio digitale le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata ed inviare ai cittadini stessi copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del Dlgs 39/1993.



- MO AFFARI ISTITUZIONALI E DI SEGRETERIA
- UO COMUNICAZ ACCREDIT RISCHIO CLIN RIC INNOVAZIONE
- UO PREVENZIONE E SICUREZZA AMBIENTI DI LAVORO
- UO PROGRAM CONTR DELLA GESTIONE E DELLA MOB SAN E COMUN
- UO ECONOMICO FINANZIARIA
- DIREZIONE DISTRETTO OVEST
- DIREZIONE DISTRETTO CENTRO NORD
- DIREZIONE DISTRETTO SUD EST
- DIREZIONE GENERALE
- DIREZIONE AMMINISTRATIVA
- DIREZIONE SANITARIA
- UO DIREZIONE INFERMIERISTICA E TECNICA
- DIREZIONE ATTIVITA SOCIO SANITARIE
- UO INGEGNERIA CLINICA
- UO DIREZIONE ATTIVITA VETERINARIE
- UO ASSISTENZA FARMACEUTICA OSP E TERRITORIALE

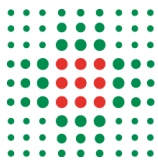
#### DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000044_2020_delibera_firmata.pdf	Carlini Stefano; Natalini Nicoletta; Vagnini Claudio	A0D34D94178DAE14946111833FEF820BB 8DDE8177A93E4C5B4FF14818286A6F5
DELI0000044_2020_Allegato1.doc:		C703A8A93B8DEF9338DD4FF37376801E BD85D3CD7D55BA90428F310684B29510



L'originale del presente documento, redatto in formato elettronico e firmato digitalmente e' conservato a cura dell'ente produttore secondo normativa vigente.

Ai sensi dell'art. 3bis c4-bis Dlgs 82/2005 e s.m.i., in assenza del domicilio digitale le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata ed inviare ai cittadini stessi copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del Dlgs 39/1993.



## **DELIBERAZIONE**

**OGGETTO:** ADOZIONE DEL DOCUMENTO: "REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI NELL'AZIENDA USL DI FERRARA (REGOLAMENTO UE 2016/679 E D.LGS. 30.06.2003 N.196) E REVOCA DELLA PROPRIA PRECEDENTE DELIBERAZIONE N. 253 DEL 28.12.2018"

### **IL DIRETTORE GENERALE**

Premesso che:

- la disciplina introdotta dal Regolamento europeo per la protezione dei dati personali, Regolamento (UE) 2016/679 (d'ora in poi GDPR), è direttamente applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018;
- la principale novità introdotta dal Regolamento consiste nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato sulla valutazione del rischio, in luogo del precedente approccio basato su adempimenti, e consegna la protezione dei dati nelle mani del Titolare del trattamento il quale, grazie al principio di responsabilizzazione, ("accountability") potrà, nei limiti e dentro i parametri delineati dal Regolamento, adottare le misure che ritiene più opportune e comprovare il conseguimento degli obiettivi che ha raggiunto nel rispetto dei principi che presidono il trattamento dei dati personali;

Dato atto peraltro che l'implementazione del "sistema privacy" delineato dal GDPR implica la necessità di generare nell'organizzazione la piena consapevolezza dei rischi inerenti ai trattamenti dei dati e le responsabilità connesse, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante della vita lavorativa dell'organizzazione, con particolare attenzione ai dati sanitari (ivi compresi i dati biometrici e genetici), nonché ai cosiddetti dati sensibili sotto il profilo dei diritti e delle libertà fondamentali dell'individuo;

Rilevato inoltre che tra gli adempimenti di maggiore importanza e di più ampio impatto, anche per le pubbliche amministrazioni, rientra certamente la designazione ed il ruolo del Data Protection Officer (DPO) o, nella versione italiana, Responsabile della Protezione dei Dati (RPD), figura prevista dall'art.37 del GDPR;

Dato atto che in tale contesto normativo e di sistema ed in linea con le indicazioni della Regione Emilia Romagna, questa Azienda UsI, unitamente all'Azienda Ospedaliera-Univ. di Ferrara, ha ritenuto opportuno procedere all'individuazione di un unico DPO esterno per entrambe le Aziende;

Rilevato che tra i primi provvedimenti a carico del sopra citato DPO vi è stato quello dell'aggiornamento delle linee guida aziendali in materia di privacy approvate con provvedimento n. 1069 del 15/12/2004;



Richiamata pertanto la vigente delibera n. 253 del 28/12/2018 recante: "Adozione del documento "Linee Guida per l'applicazione del Regolamento UE 2016/679 del D.Lgs 30.06.2003 n. 196" ed avvio del processo di accountability per l'armonizzazione dei principi disposti dal GDPR nelle Aziende sanitarie ferraresi";

Dato atto che nel corso dell'anno 2019, nello svolgimento delle attività conferite ai sensi dell'art. 37 del Regolamento UE 2016/679 (in particolare delle attività di consulenza e sorveglianza), il Data Protection Officer si è avveduto, anche relazionandosi con il Referente ICT e con il Referente del Servizio Comune Ingegneria Clinica, della necessità e dell'opportunità di proporre la modifica di talune norme contenute nelle predette Linee Guida approvate con delibera n. 253 del 28/12/2018;

Ritenuto opportuno precisare che a prescindere da alcune modifiche e/o integrazioni di natura stilistica e/o terminologica, più che altro finalizzate a rendere il testo più fruibile alla generalità dei soggetti autorizzati si è ritenuto opportuno proporre una rivisitazione sostanziale delle norme, come brevemente riassunto di seguito:

- art. 4: attribuzione ai Referenti di specifici compiti in materia di notifica e comunicazione delle violazioni dei dati (c.d. data breach) nonché dell'obbligo di popolare il Registro del Trattamento e il Registro delle Violazioni;
- art. 5 (di nuovo inserimento, ma tratto dall'attuale art. 4, comma 2 delle Linee Guida): previsione di norme specifiche applicabili al Referente del Servizio Comune ICT, più che altro finalizzate a garantire l'applicazione trasversale delle disposizioni in materia di trattamento dei dati in forma automatizzata a tutta l'Azienda, nonché previsione di norme concernenti le modalità per la distruzione e la dismissione di supporti elettronici contenenti dati personali, in linea con la prassi del Garante per la protezione dei dati personali;
- art. 6 (di nuovo inserimento, in esito a specifica proposta del Dirigente del Servizio Comune di Ingegneria Clinica): finalizzato a regolamentare con specifiche disposizioni il trattamento dei dati svolti nell'ambito dei dispositivi medici, e a regolare le modalità per la distruzione e la dismissione di supporti elettronici contenenti dati personali, in linea con la prassi del Garante per la protezione dei dati personali;
- art. 7 (attuale art. 5): imposizione ai soggetti autorizzati, oltre all'obbligo di partecipare alla formazione aziendale in materia di protezione dei dati, di prendere visione e rispettare le linee guida aziendali in materia;
- art. 12 (attuale art. 10): imposizione dell'obbligo di inserire le "informative privacy" nel sito internet aziendale, al fine di consentirne in ogni tempo la fruizione da parte degli interessati;
- art. 13 (attuale art. 11): imposizione dell'obbligo di chiedere la consulenza al DPO per il riscontro alle richieste dell'interessato;
- art. 14 (attuale art. 12): inserimento di disposizioni concernenti la modalità per la distruzione dei supporti cartacei contenenti dati personali, in linea con la prassi del Garante per la protezione dei dati personali;



- art. 17 (attuale art. 15): inserimento del divieto di utilizzo dei fax, in linea con la normativa nazionale, e previsione dell'obbligo, laddove l'utilizzo sia consentito dalla normativa, del previo parere del DPO sulla collocazione e sulla modalità di utilizzo, nonché inserimento dell'obbligo di utilizzare, per la trasmissione di documenti, il servizio cloud aziendale;

Rilevata inoltre l'opportunità, in aggiunta a quanto sopra, di modificare le attuali "Linee Guida" in "Regolamento" data la necessità, anche per conformarsi completamente al principio dell' *accountability* di cui all'art. 24 del Regolamento UE 2016/679 di adottare, successivamente, specifiche linee guida finalizzate a fornire ai soggetti autorizzati al trattamento puntuali indicazioni sulle modalità per ottemperare a singoli istituti della normativa (ad esempio: linee guida per la gestione delle violazioni di trattamento, linee guida in materia di videosorveglianza, linee guida per l'uso dei sistemi informativi aziendali, ecc.) e, quindi, anche per evitare confusioni terminologiche;

Dato atto che le predette Linee Guida, ivi comprese quelle in materia di procedura per la violazione dei dati, per la videosorveglianza, per l'uso dei sistemi informativi e della posta elettronica in ambito aziendale, ed altre, verranno adottate nei prossimi mesi, in esito a proposta del Data Protection Officer;

Vista pertanto la nota PG 10598 del 20/02/2020 con la quale il Data Protection Officer trasmette alla Direzione Strategica la proposta del "Regolamento" meglio descritto nella parte narrativa;

Richiamato il D. Lgs 33/2013 e s.m.i. recante "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" e precisato che il presente provvedimento sarà posto in pubblicazione nella sezione "Atti amministrativi generali" di "Amministrazione Trasparente";

Ritenuto, quindi, di approvare e adottare formalmente il più volte citato "Regolamento", dando altresì atto della sua dinamicità e che quindi potrà essere soggetto a variazioni anche successive alla sua adozione formale;

Dato atto che il presente provvedimento risponde ai principi della legittimità, opportunità e convenienza;

### **Delibera**

1. di provvedere all'adozione del documento "Regolamento per il trattamento dei dati personali nell'Azienda UsI di Ferrara (Regolamento UE 2016/679 e D.Lgs. 30.06.2003 n. 196)" allegato quale parte integrante e sostanziale del presente provvedimento il quale sostituisce integralmente le precedenti linee guida, approvate con la propria precedente deliberazione n. 253 del 28/12/2018;

2. di provvedere all'adeguamento dell'organizzazione aziendale disciplinando gli aspetti rimessi alla propria autonomia organizzativa e procedimentale, così come stabilito nell'allegato al presente provvedimento;



3. di prevedere un sistema di adattamento flessibile, graduale e continuativo alle disposizioni in materia, anche tenuto conto di successive disposizioni normative;

4 di trasmettere il presente provvedimento ai Direttori delle Strutture aziendali al fine della massima divulgazione all'interno delle Strutture dirette anche attraverso la pubblicazione sul sito web aziendale;

5 di prevedere la pubblicazione del presente provvedimento a cura del M.O. Affari Istituzionali e Segreteria nella sezione "Atti amministrativi generali" di "Amministrazione Trasparente" del sito istituzionale di questa Amministrazione.

Responsabile del procedimento ai sensi della L. 241/90:

Alberto Fabbri

**REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI  
NELL'AZIENDA USL DI FERRARA  
(REGOLAMENTO UE 2016/679 E D.LGS. 30.06.2003 N. 196)**

**PARTE PRIMA  
DISPOSIZIONI GENERALI**

Art. 1

**PRINCIPI GENERALI**

1. Il trattamento dei dati personali nell'ambito di ogni articolazione delle strutture dell'Azienda U.S.L. di Ferrara viene svolto garantendo a chiunque il rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
2. Il trattamento dei dati personali viene disciplinato dall'Azienda USL di Ferrara assicurando un elevato livello di tutela dei diritti e delle libertà di cui sopra nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati e per l'adempimento degli obblighi da parte del titolare del trattamento.
3. Il presente regolamento si applica al trattamento dei dati personali, anche se detenuti all'estero, effettuato dall'Azienda USL di Ferrara.

Art. 2

**TRATTAMENTO DI DATI PERSONALI**

1. Ai fini del presente atto si intende per:
  - a. **“Regolamento UE”**: il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
  - b. **“Codice”**: il decreto legislativo 30 giugno 2003 n. 196 rubricato *“Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”*;
  - c. **“DPO”**: il Responsabile della Protezione dei Dati designato dall'Azienda ai sensi degli articoli 37, 38 e 39 del Regolamento UE, contattabile all'indirizzo PEO dpo@ausl.fe.it.
2. Ai fini dell'individuazione del significato dei termini utilizzati nel presente atto si applicano le definizioni di cui all'art. 4 del Regolamento UE, di cui all'art. 2-ter e 22, comma 2, del Codice.

Art. 3

**TITOLARE E RESPONSABILE DEL TRATTAMENTO**

1. Il presente Regolamento rappresenta lo strumento con il quale l'Azienda Unità Sanitaria Locale di Ferrara specifica e fissa i compiti e le regole alle quali devono attenersi le strutture aziendali in materia di trattamento dei dati, fermo restando quanto dispongono il Regolamento UE, il Codice e le altre norme in materia di protezione dei dati.
2. Il Titolare del trattamento dei dati, anche relativamente al trattamento dei dati svolto nel contesto dell'attività libero-professionale intramuraria, è l'Azienda U.S.L. di Ferrara, persona giuridica di diritto pubblico istituita con Decreto del Presidente della Giunta della Regione Emilia Romagna n. 574 del 23.6.1994, che esercita i poteri propri del titolare per mezzo del Legale Rappresentante dell'Ente il quale può agire d'ufficio o su impulso e/o proposta del Responsabile della Protezione dei Dati.
3. L'Azienda USL, per il tramite del Direttore Generale, e con atto avente natura contrattuale, designa il Direttore Sanitario quale Responsabile del trattamento dei dati svolti per finalità di medicina preventiva, di medicina del lavoro, di valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero per finalità di gestione dei sistemi e servizi sanitari o sociali, e designa il Direttore Amministrativo quale Responsabile dei residui trattamenti svolti dall'Azienda per finalità di carattere amministrativo, attribuendo loro i compiti e le attribuzioni previste dall'art. 28 del Regolamento UE, e le funzioni di competenza del titolare del trattamento connesse al trattamento dei dati personali di loro competenza. Eventuali trattamenti con finalità sia di natura sanitaria sia di natura amministrativa vengono attribuiti alla competenza di ciascun Direttore, o di entrambi, nell'atto di designazione, con specificazione dei compiti attribuiti a ciascun Responsabile.
4. L'Azienda USL, per il tramite del Direttore Generale o dei Responsabili di cui al precedente comma 3 e/o dei Referenti di all'articolo 4, nel rispetto delle disposizioni di cui all'articolo 28 del Regolamento UE, designa inoltre responsabili del trattamento le persone fisiche e giuridiche delle quali si avvale per il trattamento dei dati, ivi compresi i soggetti che procedono al trattamento dei dati nel contesto di un servizio concesso in appalto, contratto e/o convenzione, solo se presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE e garantisca la tutela dei diritti dell'interessato. Il potere di designazione del responsabile del trattamento compete in ogni caso anche al dirigente al quale compete il potere di sottoscrizione del contratto di appalto o, comunque, dell'atto con il quale viene conferito il servizio.

#### Art. 4

##### **REFERENTI DEL TRATTAMENTO DEI DATI**

1. I Direttori di Unità Operativa e i Dirigenti titolari di strutture in staff alla direzione sono Referenti del trattamento dei dati personali, di seguito denominati "Referenti". Il Direttore Generale, nell'ambito della delibera di cui al successivo articolo 5, comma 1, o con eventuale atto integrativo successivo, può individuare altri dirigenti con funzione di Referente del trattamento dei dati personali, con specifica attribuzione dell'ambito del trattamento di competenza.
2. L'incarico di Referente viene attribuito con specifico atto al momento dell'attribuzione della funzione dirigenziale.



**3.** Fermo restando l'obbligo di vigilanza e di controllo che permane sul titolare e sul responsabile del trattamento, i Referenti, rispetto ai trattamenti di dati svolti nell'ambito della struttura di competenza, provvedono:

- a)** a garantire il pieno rispetto delle vigenti disposizioni legislative in materia di trattamento, compreso il profilo relativo alla sicurezza, e le connesse procedure aziendali da parte degli incaricati;
- b)** a fornire indicazioni e sorvegliare affinché nella struttura di sua competenza non vengano svolti trattamenti autonomi di dati e affinché non vengano trattati dati personali per finalità diverse da quelle per le quali sono stati raccolti e successivamente trattati.
- c)** a verificare la liceità e la correttezza dei trattamenti effettuati, anche attraverso controlli periodici e verificare la qualità e la quantità dei dati oggetto dei trattamenti di competenza con specifico riferimento ai requisiti di esattezza, aggiornamento, pertinenza, non eccedenza rispetto alle finalità del trattamento;
- d)** a designare, con determina, i responsabili del trattamento di cui all'art. 28 del Regolamento UE 2016/679 stipulando il contratto o l'atto giuridico di cui al medesimo art. 28, par. 3 e 4, eventualmente anche previa acquisizione del parere del DPO;
- e)** a fornire indicazioni e dare disposizioni, anche in accordo o su richiesta del DPO, per l'adeguamento alle misure di sicurezza organizzative di cui all'art. 32 del Regolamento UE 2016/679, anche provvedendo all'acquisto delle strumentazioni ritenute necessarie dal medesimo DPO;
- f)** a dare disposizioni, sulla base delle indicazioni del Titolare, del Responsabile del Trattamento o del DPO, per fornire agli interessati le informazioni di cui agli articoli 13 e 14 del Regolamento UE 2016/679;
- g)** a informare il Titolare, il Responsabile Interno e il DPO laddove sia previsto un nuovo trattamento, ai fini della valutazione della necessità e/o opportunità di provvedere alla valutazione di impatto ai sensi dell'art. 35 del Regolamento, alla consultazione preventiva ai sensi dell'art. 36 del Regolamento e alla predisposizione del registro dei trattamenti ai sensi dell'art. 30 del Regolamento, e collaborare con i medesimi alla sua predisposizione;
- h)** a informare il Titolare, il Referente Servizio Comune ICT e il DPO, entro 12 ore da quando ne è venuto a conoscenza, dell'avvenuta violazione dei dati personali di cui all'articolo 33 del Regolamento UE, provvedendo alla predisposizione dell'atto di notifica al Garante per la protezione dei dati personali, alla predisposizione della comunicazione agli interessati di cui all'art. 34 del Regolamento UE, e alla registrazione dell'evento nel Registro delle violazioni, il tutto nel rispetto delle linee guida aziendali in materia e, comunque, avvalendosi della consulenza, se necessario, del DPO;
- i)** collaborare con il Referente del Servizio Comune ICT e/o con il DPO, secondo le loro indicazioni, ai fini dell'aggiornamento del Registro delle Attività di trattamento;
- j)** provvedere ad ogni altro atto o adempimento necessario per l'applicazione ai trattamenti di dati dell'Azienda del Regolamento UE 2016/679 e di ogni altra norma in materia, europea e nazionale, anche in relazione alle indicazioni del Titolare, del Responsabile del Trattamento o DPO, collaborando a tal fine con

quest'ultimo e, ai sensi dell'art. 31 del Regolamento, con il Garante per la protezione dei dati.

#### Art. 5

#### **REFERENTE DEL SERVIZIO COMUNE ICT**

**1.** Al responsabile della struttura denominata Servizio Comune ICT, già nominato Referente interno del trattamento ai sensi del precedente articolo 4, sono attribuiti, altresì, i seguenti compiti:

- a)** sovrintendere alle risorse del sistema informatico centralizzato (software dipartimentali e trasversali) e consentirne l'utilizzazione a tutti i responsabili e gli incaricati che ne abbiano titolo, mediante l'adozione delle misure di sicurezza tecniche di cui all'art. 32 del Regolamento UE;
- b)** garantire la gestione e manutenzione degli strumenti elettronici aziendali;
- c)** garantire la protezione dei dispositivi e dei programmi contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
- d)** garantire gli aggiornamenti periodici, almeno con cadenza annuale, dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati particolari l'aggiornamento deve essere svolto almeno semestralmente;
- e)** impartire istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno quotidiana e, comunque, che garantiscano tempestivamente il ripristino, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- f)** adottare idonee misure che assicurino l'integrità e la disponibilità dei dati;
- g)** adottare idonee misure che assicurino il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;
- h)** in caso di trattamento di dati particolari, predisporre misure di pseudonimizzazione e cifratura dei dati personali, anche garantendo il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati;
- i)** predisporre misure di sicurezza finalizzate a garantire che la dismissione e la distruzione dei supporti che contengono dati personali avvenga nel rispetto del provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008, pubblicato in G.U. n. 287 del 9 dicembre 2008;
- j)** procedere alla notifica al Garante per la protezione dei dati personali dei modelli di notifica comunicatigli dai Referenti ai sensi del precedente articolo, lett. h);
- k)** costituire, aggiornare e conservare il Registro delle attività del trattamento, eventualmente previa consultazione con il DPO, anche dando indicazioni ai Referenti per la trasmissione delle informazioni necessarie per l'aggiornamento del Registro stesso;
- l)** costituire, aggiornare e conservare il Registro della violazione dei dati personali, eventualmente previa consultazione con il DPO, anche dando

- indicazioni ai Referenti per la trasmissione delle informazioni necessarie per l'aggiornamento del Registro stesso;
- m) procedere, laddove ritenuto necessario e/o opportuno da lui medesimo, o dal DPO, alla valutazione di impatto di cui all'articolo 35 del Regolamento UE, avvalendosi della consulenza del medesimo Responsabile, avvisando il Titolare laddove derivi la necessità di procedere alla consultazione preventiva di cui all'articolo 36 del Regolamento UE;
  - n) implementare ogni misura finalizzata al rispetto del disciplinare interno sull'uso dei sistemi informativi.
2. Tenuto conto del fatto che l'accesso ai dati e alle procedure aziendali è consentito, per necessità di operatività e sicurezza dei sistemi, ai soggetti autorizzati del Servizio Comune ICT cui sono attribuite le caratteristiche di superutente, il responsabile del Servizio Comune ICT procede all'individuazione del preposto all'intervento sui sistemi e procedure aziendali in assenza dei soggetti autorizzati al trattamento, se pur nel rispetto del disciplinare interno in materia di uso dei sistemi informativi.

#### Art. 6

##### **REFERENTE DEL SERVIZIO COMUNE DI INGEGNERIA CLINICA**

1. Al responsabile della struttura denominata Servizio Comune Ingegneria Clinica, già nominato Referente interno del trattamento ai sensi del precedente articolo 4, sono attribuiti, altresì, i seguenti compiti:
- a) sovrintendere alle risorse dei programmi per elaboratore qualificati e/o certificati Dispositivi Medici (in breve DM) e consentirne l'utilizzazione a tutti i responsabili e gli incaricati che ne abbiano titolo, mediante l'adozione delle misure di sicurezza tecniche di cui all'art. 32 del Regolamento UE;
  - b) garantire la gestione e manutenzione dei programmi DM siano essi integrati nelle tecnologie biomediche oppure accessori di tecnologie biomediche oppure autonomi e indipendenti da qualsivoglia tecnologia (cosiddetti stand alone);
  - c) garantire la protezione dei programmi DM contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare la cadenza ritenuta necessaria in conformità all'art. 32 del Regolamento UE;
  - d) garantire gli aggiornamenti periodici dei programmi DM al fine di prevenirne la vulnerabilità secondo la periodicità ritenuta necessaria in conformità all'art. 32 del Regolamento UE;
  - e) impartire istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con la periodicità ritenuta necessaria in conformità all'art. 32 del Regolamento UE al fine di garantire tempestivamente il ripristino, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  - f) promuovere l'adozione di idonee misure che assicurino l'integrità e la disponibilità dei dati;
  - g) promuovere l'adozione di idonee misure che assicurino il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e comunque non superiori a tre giorni;

- h) predisporre misure di sicurezza finalizzate a garantire che la dismissione e la distruzione dei supporti che contengono dati personali avvenga nel rispetto del provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008, pubblicato in G.U. n. 287 del 9 dicembre 2008;
  - i) in caso di trattamento di dati particolari predisporre misure di pseudonimizzazione e cifratura dei dati personali, anche garantendo il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati;
  - j) contribuire con il Referente ICT alla redazione e all'aggiornamento del Registro delle attività del trattamento e del Registro delle violazioni dei dati personali, eventualmente previa consultazione con il DPO;
  - k) procedere, laddove ritenuto necessario e/o opportuno da lui medesimo, o dal DPO, alla valutazione di impatto di cui all'articolo 35 del Regolamento UE, avvalendosi della consulenza del medesimo DPO o, comunque, chiedendo, in esito, il parere di quest'ultimo, ed avvisando il Titolare laddove derivi la necessità di procedere alla consultazione preventiva di cui all'articolo 36 del Regolamento UE.
2. L'individuazione delle misure di sicurezza è svolta unitamente al Referente ICT in relazione ai criteri individuati dall'Agenzia per l'Italia Digitale e, comunque, in conformità a quanto disposto dall'art. 32 del Regolamento UE.
3. La tipologia di dati trattati e le modalità del trattamento sono identificati mediante la compilazione di specifica modulistica all'atto dell'ingresso di una tecnologia biomedica o programma DM.

#### Art. 7

##### **AUTORIZZAZIONE AL TRATTAMENTO DEI DATI**

1. Ai fini dell'autorizzazione al trattamento prevista dall'art. 2-quaterdecies del d.lgs. 196/03, con delibera del Direttore Generale viene individuato, per ciascuno dei trattamenti di dati descritti nel Registro delle Attività di Trattamento di cui all'art. 30 del Regolamento UE, il dipartimento, l'unità operativa e/o la struttura di staff alle quali è attribuito il trattamento stesso, con possibilità di prevedere specifici trattamenti di dati di competenza delle sole strutture semplici (M.O.).
2. La preposizione dei dipendenti e di coloro che a diverso titolo devono trattare i dati personali nel contesto di ciascuna delle predette strutture aziendali deve essere effettuata dal servizio comune gestione del personale all'atto dell'assunzione o del trasferimento e/o mutamento di mansioni, e tale preposizione costituisce atto autorizzativo al relativo trattamento ai sensi degli articoli 29 del Regolamento UE e 2-quaterdecies del Codice.
3. I soggetti autorizzati al trattamento sono tenuti a prendere visione e rispettare le istruzioni e le linee guida in materia di trattamento dei dati personali pubblicati nella intranet dell'Azienda e a partecipare agli incontri e alle iniziative di formazione organizzati periodicamente e/o indicati dal Titolare e dai Responsabili del trattamento sulla base delle indicazioni fornite dal DPO, anche per il tramite del Servizio Interaziendale Formazione e Aggiornamento.
4. I singoli soggetti autorizzati, anche se esercenti attività libero professionale intramuraria, sono tenuti a svolgere il trattamento dei dati personali esclusivamente utilizzando gli applicativi dell'Azienda.

## ART. 8

### **COMUNICAZIONE AL GARANTE**

1. I singoli referenti di cui all'articolo 3 sono tenuti ad avvisare il Titolare e/o il Responsabile del Trattamento di competenza, ai fini della comunicazione al Garante per la protezione dei dati personali di cui all'art. 2-ter, comma 2, secondo periodo, del Codice, laddove debbano procedere alla comunicazione di dati personali che non sia consentita dall'art. 2-ter, comma 2, primo periodo, del Codice.
2. I singoli referenti di cui all'articolo 3 sono tenuti a dare previo avviso all'ufficio ricerca di competenza laddove debbano procedere al trattamento dei dati particolari per finalità di ricerca scientifica al fine di verificare il rispetto delle disposizioni in materia di trattamento dei dati per tali finalità.

## ART. 9

### **MODALITA' DI RACCOLTA E REQUISITI DEI DATI**

1. I Responsabili, i Referenti e i soggetti autorizzati al trattamento sono tenuti a trattare i dati nel rispetto delle disposizioni di cui all'articolo 5 del Regolamento UE.
2. Ciascun soggetto autorizzato è tenuto a raccogliere e registrare i dati da trattare in forma automatizzata attraverso gli strumenti elettronici messi a disposizione dall'azienda, invitando il paziente e/o l'utente ad esibire la tessera sanitaria europea, anche nel caso in cui l'erogazione della prestazione sanitaria sia preceduta dalla prenotazione.
3. Ciascun soggetto autorizzato è tenuto a identificare i pazienti e/o gli utenti al momento dell'erogazione di ciascuna prestazione.

## ART. 10

### **INFORMATIVA PER I TRATTAMENTI EFFETTUATI AI SOLI FINI AMMINISTRATIVI**

1. L'Azienda USL di Ferrara può trattare i dati personali per fini amministrativi esclusivamente ai fini di cui all'articolo 6, par. 2, lettera e) del Regolamento UE, ovvero quanto è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita l'Azienda, e ai fini dell'articolo 9, par. 2, lett g) del medesimo Regolamento, ovvero quando il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.
2. I Referenti sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli articoli 13 e 14 del Regolamento UE nel rispetto delle indicazioni fornite dal Responsabile del trattamento di competenza e/o dal DPO.
3. I Responsabili del trattamento, per i trattamenti di rispettiva competenza, anche su proposta del DPO, curano che le informazioni di cui al comma 1 siano rese note anche mediante pubblicazione nel sito internet aziendale.

## ART. 11

### **INFORMATIVA RELATIVA AL TRATTAMENTO DEI DATI CONNESSO AL RAPPORTO CONTRATTUALE, LAVORATIVO, PROFESSIONALE, AUTONOMO E CONVENZIONALE**

1. L'Azienda USL di Ferrara può inoltre trattare i dati per i fini di cui all'articolo 6, par. 2, lett. b) del Regolamento UE, ovvero quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, nonché per i fini di cui all'art. 6, par. 2, lett. b) del medesimo Regolamento UE, ovvero quando il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.
2. I Referenti sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli articoli 13 e 14 del Regolamento UE nel rispetto delle indicazioni fornite dal Titolare, Responsabile del trattamento di competenza e/o dal DPO. In ogni caso le predette informazioni dovranno essere inserite nei relativi atti contrattuali e, laddove il rapporto sia soggetto a procedure concorsuali, le predette informazioni dovranno essere necessariamente contenute nei bandi di concorso, di gara, nelle lettere di invito e/o avvisi pubblici.
3. I responsabili del trattamento, per i trattamenti di rispettiva competenza, anche su proposta del DPO, curano che le informazioni di cui al comma 1 siano rese note anche mediante pubblicazione nel sito internet aziendale.

## ART. 12

### INFORMATIVE VARIE

1. I referenti, secondo i relativi settori di competenza, provvedono a rendere le informazioni di cui agli articoli 13 e 14 del Regolamento UE secondo le indicazioni fornite dal DPO e, comunque, a titolo esemplificativo:
  - a. in materia di attività dell'U.O. Medicina Legale consegnando la specifica modulistica messa a disposizione dall'Azienda al momento della presentazione della richiesta di prestazione o, salvo diversa indicazione del DPO, al momento di primo contatto con il paziente;
  - b. in materia di attività dell'URP consegnando la specifica modulistica messa a disposizione dall'Azienda unitamente alla consegna dei moduli messi a disposizione per la segnalazione;
  - c. in materia di recupero crediti del dipendente a seguito di infortuni in itinere o infermità causata da terzi consegnando o inviando la specifica modulistica messa a disposizione dall'Azienda;
  - d. in materia di responsabilità civile di terzi consegnando o inviando la specifica modulistica messa a disposizione dall'Azienda al momento della comunicazione dell'apertura del sinistro;
  - e. in materia di riconoscimento dell'assegno una tantum o dell'assegno reversibile di cui alla legge 210/92, dell'indennizzo correlato a vaccinazione, trasfusione o somministrazione di emoderivati, consegnando la specifica modulistica messa a disposizione dall'Azienda unitamente alla consegna dei moduli messi a disposizione per la richiesta;
  - f. in materia di valutazione delle necessità assistenziali nell'ambito delle attività socio-sanitarie integrate, consegnando la specifica modulistica messa a disposizione dall'Azienda unitamente alla consegna dei moduli messi a disposizione per la segnalazione.

2. In ogni caso i Referenti saranno tenuti a seguire le indicazioni eventualmente fornite dal DPO, che potranno anche derogare agli obblighi di cui al precedente comma.
3. In ogni caso i Referenti avranno cura di inserire le predette informative nel sito internet dell'Azienda.

#### ART. 13

##### **DIRITTI DELL'INTERESSATO**

1. L'interessato che eserciti i diritti previsti dagli articoli 15 e seguenti del Regolamento UE dovrà essere identificato sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura o di delega sottoscritta dall'interessato nelle forme di cui all'articolo 38 del DPR 445/00.
2. L'eventuale richiesta verbale da parte dell'interessato dovrà essere annotata a cura del Referente e/o del personale autorizzato.
3. Il personale autorizzato che riceva una richiesta di cui agli articoli 15 e seguenti del Regolamento UE è tenuto a trasmetterla entro 2 giorni al referente del trattamento dei dati, salvo che non sia addetto specificamente al servizio che comporta, per disposizioni interne, il riscontro alla specifica richiesta.
4. Il referente che abbia dubbi sulle modalità per provvedere al riscontro alla richiesta dell'interessato è tenuto a inoltrare la relativa richiesta al DPO entro 5 giorni dalla sua ricezione al fine di ottenerne la sua consulenza sul contenuto e sulla modalità del riscontro.

#### ART. 14

##### **MISURE DI SICUREZZA**

1. Il Referente e il personale autorizzato sono tenuti:
  - a. a trattare i soli dati essenziali per svolgere l'attività istituzionale riducendo al minimo l'utilizzo di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi, dati di natura meno invasiva od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
  - b. a introdurre e controllare i dati in modo da ridurre al minimo i rischi di distruzione e perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla qualità della raccolta, tramite l'applicazione di misure di sicurezza adottate dal Servizio Comune ICT e/o del DPO in conformità all'articolo 32 del Regolamento UE ed anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, secondo le indicazioni impartite dal Servizio Comune ICT e/o dal DPO.
2. I dati su supporto cartaceo dovranno essere conservati in luoghi e contenitori atti ad evitare perdite, sottrazioni, danneggiamenti, distruzioni e l'accesso a soggetti diversi dal personale autorizzato al relativo trattamento, nel rispetto peraltro del principio della tutela della riservatezza di terzi.

3. Il personale autorizzato ha accesso ai soli dati la cui conoscenza sia direttamente necessaria per adempiere ai compiti loro assegnati.
4. Gli atti e i documenti devono essere conservati in archivi ad accesso selezionato e gli incaricati debbono conservarli e restituirli al termine delle operazioni effettuate.
5. Nel caso di trattamenti di dati particolari di cui agli articoli 9 e 10 del Regolamento UE, oltre a quanto sopra previsto debbono essere osservate le seguenti modalità:
  - a. gli atti e documenti debbono essere conservati in locali o contenitori muniti di serratura, fino alla loro eventuale distruzione nel rispetto dei limiti temporali previsti dalle norme in materia di scarto degli atti d'archivio;
  - b. l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi accedono dopo l'orario di chiusura degli archivi stessi.
6. Ciascun referente del trattamento dovrà individuare e rappresentare all'Azienda o al Responsabile della protezione dei dati l'insieme dei beni materiali necessari per garantire la sicurezza dei dati trattati su supporto cartaceo nelle proprie articolazioni di competenza.
7. Per ogni singolo trattamento di dati deve essere individuata la finalità e la compatibilità con i fini istituzionali. I trattamenti di dati raccolti e conservati per espressa disposizione normativa deve essere specificata la relativa fonte normativa.
8. I Referenti, anche mediante controlli periodici, sono tenuti a verificare costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto e alla prestazione in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.
9. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.
10. Il trattamento dei dati, anche particolari, effettuato con strumenti elettronici è consentito solo se sono adottate le seguenti misure minime garantite dal Servizio Comune ICT:
  - a. autenticazione informatica, con le specifiche procedure di gestione delle credenziali di autenticazione;
  - b. utilizzazione di un sistema di autorizzazione;
  - c. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito al personale autorizzato e agli addetti alla gestione o alla manutenzione degli strumenti elettronici;
  - d. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
  - e. adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
  - f. adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale.
11. I documenti cartacei che contengano dati personali e dei quali non sia imposta la conservazione devono essere smaltiti attraverso appositi



distruggidocumenti o, se non disponibili, distruggendo fisicamente il supporto cartaceo in modo che ne sia impedita la ricostruzione.

**12.** La distruzione di ingenti quantità di documenti cartacei deve essere effettuata, in accordo con il Referente, attraverso l'incarico ad esperti del settore (es. società di smaltimento rifiuti) che dovranno essere designati alla responsabilità del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679.

#### ART. 15

### **COMUNICAZIONE DI DATI PERSONALI**

**1.** Fermo restando quanto previsto dalle norme di cui al Regolamento UE e al Codice, non configura comunicazione dei dati il trasferimento degli stessi alle diverse strutture dell'Azienda USL di Ferrara.

#### ART.16

### **TRATTAMENTO DEI DATI NEGLI ATTI SOGGETTI A PUBBLICAZIONE**

**1.** Gli atti dell'Azienda soggetti a pubblicazione contenenti dati particolari di cui agli articoli 9 e 10 del Regolamento UE, i provvedimenti disciplinari e gli atti concernenti i minori, non dovranno essere pubblicati in forma identificativa

**2.** Sarà cura dei Referenti valutare le modalità per pseudoanonimizzarli, eventualmente previa consultazione con il DPO, garantendo in ogni caso al diretto interessato la possibilità di identificarsi.

## **PARTE SECONDA**

### **TRATTAMENTO DI DATI PERSONALI E PARTICOLARI PER FINALITA' DI DIAGNOSI, ASSISTENZA, TERAPIA SANITARIA O SOCIALE**

#### ART. 17

### **MODALITA' SEMPLIFICATE PER L'INFORMATIVA AL PAZIENTE**

**1.** Con riferimento al trattamento dei dati per finalità di diagnosi, assistenza, terapia sanitaria o sociale l'Azienda USL è tenuta a rendere le informazioni previste dagli articoli 13 e 14 del Regolamento UE secondo le modalità concordate con il DPO.

**2.** In ogni caso tali informazioni dovranno essere fornite, anche sinteticamente ma con rinvio al sito internet aziendale, al momento della richiesta di accesso alla presentazione sanitaria nonché attraverso specifica cartellonistica situata nelle zone di accesso, transito e attesa dei pazienti.

**3.** Per i ricoveri ospedalieri una copia della modulistica contenente l'informativa in forma semplificata dovrà essere consegnata unitamente alla consegna della modulistica necessaria per la preparazione dell'intervento.

**4.**

#### ART. 18

### **MODALITA' PARTICOLARI DEL TRATTAMENTO DEI DATI**

**1.** Al fine di garantire il rispetto dei diritti, delle libertà fondamentali, della dignità, della riservatezza e della protezione dei dati degli interessati, nonché del segreto professionale, all'interno di ogni struttura erogatrice di prestazioni sanitarie dell'Azienda USL di Ferrara sono adottate misure operative, anche previa

consultazione o su indicazione del DPO, atte a garantire la protezione dei dati, tra le quali:

- a. soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
  - b. l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;
  - c. soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
  - d. cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
  - e. il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;
  - f. la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;
  - g. la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, rispettando eventuali contrarie manifestazioni di volontà da parte degli interessati;
  - h. la messa in atto di procedure dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
  - i. la sottoposizione del personale autorizzato, che sia tenuto per legge al segreto professionale, a regole di condotta analoghe al segreto professionale.
- 2.** I referti degli esami specialistici dovranno essere compilati in due copie di cui, una, contenente la diagnosi, da consegnare in busta chiusa all'interessato o suo delegato, e un'altra non contenente alcun riferimento diagnostico, da poter utilizzare nei relativi procedimenti amministrativi.
- 3.** Fermo restando quanto previsto al comma 1, i dati idonei a rivelare lo stato di salute possono essere resi noti agli interessati solo per il tramite di un medico designato dall'interessato o dall'Azienda.
- 4.** La copia della cartella clinica e di altra documentazione sanitaria deve essere consegnata all'interessato o a persona munita di apposita delega sottoscritta dall'interessato stesso e autenticata nelle forme di cui all'art. 38 del DPR 445/2000.
- 5.** Eventuali richieste di presa visione o di rilascio di copia della cartella clinica o dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:
- a. di far valere o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato e, quindi, consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile;

b. di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato o consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

6. Le ricette farmaceutiche dovranno essere redatte in modo tale da poter risalire all'identità dell'interessato solo in caso di necessità connesse al controllo della prescrizione ovvero ai fini di verifiche amministrative o per scopi epidemiologici o di ricerca tali da escludere la necessità delle generalità dell'interessato.

7. Le ricette contenenti prescrizioni relative a stupefacenti e sostanze psicotrope, di cui deve essere accertata l'identità dell'interessato, devono essere conservate separatamente da ogni altro documento che non ne richiede l'utilizzo.

#### ART. 19

##### **ALTRE MISURE OPERATIVE IN MATERIA DI DATI PARTICOLARI**

1. E' fatto divieto di fornire indicazioni inerenti lo stato di salute degli interessati per via telefonica o telematica.

2. E' fatto divieto di utilizzo degli apparecchi fac-simile. Laddove l'uso dei singoli apparecchi sia strettamente necessario, e consentito dalla normativa vigente, il Referente del trattamento ne informa il DPO che fornirà indicazioni per la trasmissione e la ricezione delle comunicazioni e affinché la relativa apparecchiatura sia collocata in un'area protetta e presidiata.

3. Nei casi di cui al comma 2, il Referente cura che, nel caso si debba procedere alla comunicazione di dati particolari tramite fax con un ente esterno autorizzato per legge all'acquisizione di tale documentazione, laddove ne sia consentito l'utilizzo, si concordi un numero di fax non accessibile a terzi da utilizzare sempre e in modo esclusivo per tale comunicazione. Ciascuna comunicazione dovrà essere preceduta da una copertina nella quale non siano inclusi dati personali particolari né dati personali di soggetti diversi dal mittente e dal destinatario.

4. Il personale autorizzato è tenuto al ritiro tempestivo della documentazione dalla stampante e dalla fotocopiatrice contenente dati personali ed alla conservazione della stessa. In tali casi è comunque fatto divieto di utilizzare supporti cartacei che contenga già informazioni personali e sensibili sull'altro lato del foglio.

5. La trasmissione interna ed esterna di corrispondenza e di documentazione contenente dati particolari dovrà essere effettuata attraverso il servizio "cloud" aziendale o, se non è possibile, dovrà essere effettuata necessariamente in busta chiusa e sigillata che riporti il nominativo del destinatario.

6. L'accesso alle immagini registrate dagli impianti di videosorveglianza è consentita al personale specificamente autorizzato dal referente del trattamento.

7. Laddove necessario per finalità di diagnosi e terapia o per la corretta alimentazione del paziente, le domande relative alla convinzione religiosa dell'interessato devono essere formulate in modo generico tale da non arrecare pregiudizio e disagio allo stesso.

#### ART. 20

##### **DISPOSIZIONE FINALE**

1. Ogniquale volta sussistano dubbi sulla applicazione della normativa in materia di protezione dei dati personali, del presente Regolamento e/o delle altre linee guida

eventualmente approvate dall'Azienda in applicazione di specifiche questioni di cui al presente Regolamento, il personale autorizzato è tenuto ad attenersi al criterio della tutela e del massimo rispetto della riservatezza nei confronti dell'interessato e di massima protezione dei dati personali, pur garantendo nel contempo il normale espletamento delle attività.

**2.** In ogni caso il personale autorizzato è tenuto, nei casi di cui al comma 1, a rivolgersi al Referente del trattamento di competenza il quale, nel caso, può chiedere consulenza, per via telematica, al DPO.

**3.** Per tutto quanto non espressamente previsto dal presente Regolamento si applicano le disposizioni del Regolamento UE e del Codice, nonché le pertinenti disposizioni amministrative.